



# Software Diversification for WebAssembly

JAVIER CABRERA-ARTEAGA

Doctoral Thesis in Computer Science  
Supervised by  
Benoit Baudry and Martin Monperrus  
Stockholm, Sweden, 2023

KTH Royal Institute of Technology  
School of Electrical Engineering and Computer Science  
Division of Software and Computer Systems  
SE-10044 Stockholm  
Sweden

TRITA-EECS-AVL-2020:4  
ISBN 100-

Akademisk avhandling som med tillstånd av Kungl Tekniska högskolan framlägges  
till offentlig granskning för avläggande av Teknologie doktorexamen i elektroteknik  
i .

© Javier Cabrera-Arteaga , date

Tryck: Universitetsservice US AB

## **Abstract**

**Keywords:** Lorem, Ipsum, Dolor, Sit, Amet

## **Sammanfattning**

# LIST OF PAPERS

1. ***WebAssembly Diversification for Malware Evasion***  
**Javier Cabrera-Arteaga**, Tim Toady, Martin Monperrus, Benoit Baudry  
*Computers & Security, Volume 131, 2023, 17 pages*  
<https://www.sciencedirect.com/science/article/pii/S0167404823002067>
2. ***Wasm-mutate: Fast and Effective Binary Diversification for WebAssembly***  
**Javier Cabrera-Arteaga**, Nicholas Fitzgerald, Martin Monperrus, Benoit Baudry  
*Under review, 17 pages*  
<https://arxiv.org/pdf/2309.07638.pdf>
3. ***Multi-Variant Execution at the Edge***  
**Javier Cabrera-Arteaga**, Pierre Laperdrix, Martin Monperrus, Benoit Baudry  
*Moving Target Defense (MTD 2022), 12 pages*  
<https://dl.acm.org/doi/abs/10.1145/3560828.3564007>
4. ***CROW: Code Diversification for WebAssembly***  
**Javier Cabrera-Arteaga**, Orestis Floros, Oscar Vera-Pérez, Benoit Baudry, Martin Monperrus  
*Measurements, Attacks, and Defenses for the Web (MADWeb 2021), 12 pages*  
<https://doi.org/10.14722/madweb.2021.23004>
5. ***Superoptimization of WebAssembly Bytecode***  
**Javier Cabrera-Arteaga**, Shrinish Donde, Jian Gu, Orestis Floros, Lucas Satabin, Benoit Baudry, Martin Monperrus  
*Conference Companion of the 4th International Conference on Art, Science, and Engineering of Programming (Programming 2021), MoreVMs, 4 pages*  
<https://doi.org/10.1145/3397537.3397567>
6. ***Scalable Comparison of JavaScript V8 Bytecode Traces***  
**Javier Cabrera-Arteaga**, Martin Monperrus, Benoit Baudry  
*11th ACM SIGPLAN International Workshop on Virtual Machines and Intermediate Languages (SPLASH 2019), 10 pages*  
<https://doi.org/10.1145/3358504.3361228>



# ACKNOWLEDGEMENT





# Contents

<b>List of Papers</b>	<b>iii</b>
<b>Acknowledgement</b>	<b>v</b>
<b>Contents</b>	<b>1</b>
<b>I Thesis</b>	<b>3</b>
<b>1 Introduction</b>	<b>5</b>
1.1 Background . . . . .	5
1.2 Problem statement . . . . .	5
1.3 Automatic Software diversification requirements . . . . .	5
1.4 List of contributions . . . . .	6
1.5 Summary of research papers . . . . .	6
<b>2 Background and state of the art</b>	<b>9</b>
2.1 WebAssembly . . . . .	9
2.1.1 From source code to WebAssembly . . . . .	10
2.1.2 WebAssembly’s binary format . . . . .	12
2.1.3 WebAssembly’s runtime . . . . .	13
2.1.4 WebAssembly’s control-flow . . . . .	15
2.1.5 Security and Reliability for WebAssembly . . . . .	16
2.1.6 Open challenges . . . . .	18
2.2 Software diversification . . . . .	19
2.2.1 Generation of Software Variants . . . . .	19
2.2.2 Variants deployment . . . . .	22
2.2.3 Open challenges . . . . .	24
<b>3 Automatic Software Diversification for WebAssembly</b>	<b>27</b>

3.1	CROW: Code Randomization of WebAssembly . . . . .	28
3.1.1	Enumerative synthesis . . . . .	29
3.1.2	Constant inferring . . . . .	30
3.1.3	Exemplifying CROW . . . . .	31
3.2	MEWE: Multi-variant Execution for WebAssembly . . . . .	33
3.2.1	Multivariant call graph . . . . .	34
3.2.2	Exemplifying a Multivariant binary . . . . .	34
3.3	WASM-MUTATE: Fast and Effective Binary for WebAssembly . . . . .	37
3.3.1	WebAssembly Rewriting Rules . . . . .	38
3.3.2	E-Graphs traversals . . . . .	39
3.3.3	Exemplifying WASM-MUTATE . . . . .	40
3.4	Comparing CROW, MEWE, and WASM-MUTATE . . . . .	42
3.4.1	Security applications . . . . .	45
<b>4</b>	<b>Exploiting Software Diversification for WebAssembly</b>	<b>47</b>
4.1	Offensive Diversification: Malware evasion . . . . .	47
4.1.1	Threat model: cryptojacking defense evasion . . . . .	48
4.1.2	Methodology . . . . .	49
4.1.3	Results . . . . .	51
4.2	Defensive Diversification: Speculative Side-channel protection . . . . .	55
4.2.1	Threat model: speculative side-channel attacks . . . . .	56
4.2.2	Methodology . . . . .	57
4.2.3	Results . . . . .	58
<b>5</b>	<b>Conclusions and Future Work</b>	<b>65</b>
5.1	Summary of technical contributions . . . . .	65
5.2	Summary of empirical findings . . . . .	65
5.3	Future Work . . . . .	65
<b>II</b>	<b>Included papers</b>	<b>67</b>
	Superoptimization of WebAssembly Bytecode	<b>71</b>
	CROW: Code Diversification for WebAssembly	<b>73</b>
	Multi-Variant Execution at the Edge	<b>75</b>
	WebAssembly Diversification for Malware Evasion	<b>77</b>
	Wasm-mutate: Fast and Effective Binary Diversification for WebAssembly	<b>79</b>
	Scalable Comparison of JavaScript V8 Bytecode Traces	<b>81</b>

Part I

Thesis

